

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号
特開2002-281573
(P2002-281573A)

(43)公開日 平成14年9月27日(2002.9.27)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード*(参考)
H 0 4 Q 9/00	3 2 1	H 0 4 Q 9/00	3 2 1 E 5 B 0 5 8
	3 0 1		3 0 1 C 5 C 0 8 7
G 0 6 K 17/00		G 0 6 K 17/00	L 5 K 0 4 8
G 0 8 B 25/04		G 0 8 B 25/04	F 5 K 1 0 1
H 0 4 M 11/00	3 0 1	H 0 4 M 11/00	3 0 1

審査請求 未請求 請求項の数3 O L (全 10 頁)

(21)出願番号 特願2001-78703(P2001-78703)

(22)出願日 平成13年3月19日(2001.3.19)

(71)出願人 000232047

日本電気エンジニアリング株式会社

東京都港区芝浦三丁目18番21号

(72)発明者 島津 典彦

東京都港区芝浦三丁目18番21号 日本電気
エンジニアリング株式会社内

(74)代理人 100082935

弁理士 京本 直樹 (外2名)

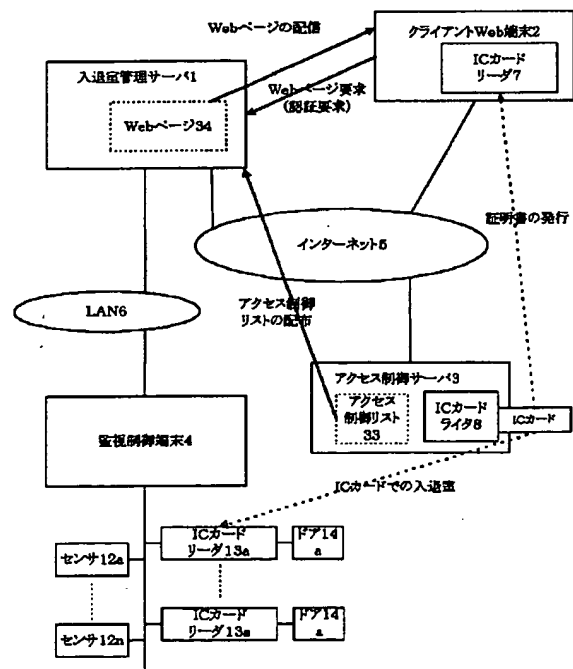
最終頁に続く

(54)【発明の名称】 インターネットを利用した遠隔監視方法及び、遠隔監視システム。

(57)【要約】

【課題】入退室管理システムにおいて、遠隔地からの状態監視を可能とした上で、クライアント装置から、サーバ装置への不正アクセスを防止し、セキュリティ性の高いシステムを提供する。

【解決手段】入退室管理サーバにWebサーバを登録し、インターネットに接続し、クライアントWeb端末からの遠隔状態監視を可能とする。また、クライアントWeb端末からWebサーバへのクライアント認証に、ICカード内の証明書を用いることで、不正アクセスに対するセキュリティ性を向上させた。



【特許請求の範囲】

【請求項1】 管理サーバ端末は、監視制御装置が収集する監視対象物の各種状態変化情報を蓄積し、これと通信接続されたクライアント端末にて前記管理サーバ端末から配信された前記各種状態変化情報を表示することで監視対象物の遠隔監視を行う遠隔監視制御システムにおいて、前記管理サーバ端末と前記クライアント端末をインターネット接続し、ユーザ固有の個人情報証明書をデータとして書き込んだICカードを発行し、この証明書データを前記管理サーバ端末に送信するICカード発行手段と、前記クライアント端末は、前記ICカードを読み取る手段と、前記管理サーバに対するインターネット接続時にICカードから読みとった証明書データを前記管理サーバに送信する手段とを含み、前記管理サーバは、前記各種状態変化情報に基づきWebページを生成する手段と、前記ICカード発行手段から受信した証明書データに基づき各ユーザに対してアクセス権限を割り当てる手段と、このアクセス権限に基づき前記Webページの配信の可否を決定する手段とを含み、前記クライアント端末より前記ICカードから読みとった証明書データの送信を伴う前記管理サーバに対するインターネット接続が実行されると、前記管理サーバは、受信したユーザの証明書データから前記アクセス権限を参照して当該ユーザに認められるWebページのみを前記クライアント端末に送出することを特徴とする遠隔監視制御システム。

【請求項2】 請求項1において、前記クライアント端末は、前記管理サーバ端末の各Webページへのアクセス要求毎に、前記ICカードから読み込んだ証明書データを前記管理サーバ端末に送信し、前記管理サーバは、受信した証明書データを元に前記アクセス権限を参照することでWebページにアクセスしようとしているユーザを特定し、特定したユーザが、要求されたWebページに対してアクセスを許可されている場合にのみWebページを要求元のクライアント端末に配信することを特徴とする遠隔監視制御システム。

【請求項3】 請求項1～2記載の遠隔監視制御システムにおいて、前記管理サーバ端末から前記クライアント端末に配信されるWebページは、HTML(Hyper Text Markup Language)形式またはASP(Active Server Pages)形式によって記述されていることを特徴とする遠隔監視制御システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、インターネットやイントラネットを利用した遠隔状態監視システムに関する

【0002】

【従来の技術】 従来の遠隔監視制御システムとしては、例えば特開2000-11280号公報が知られている。公報に記載の発明は、センサによる侵入者や火災の警報、ドア毎に設けられたカードリーダによる入室退室の制限、センサ発報や入室退室の履歴の記録等の機能を持ち、主に機密性を必要とするビルや工場に設置される。

【0003】 複数のセンサやカードリーダは、監視制御端末に通信ラインにより接続され、異常感知によるセンサ発報通知や、カードリーダ操作によるドア開放閉鎖等は、監視制御端末によりリアルタイムに制御が行われており、同時に履歴の記録も監視制御端末により行われている。

【0004】 監視制御端末と、監視制御端末に接続されたセンサ、カードリーダだけでも小規模な入室退室管理システムとして構成できるが、中・大規模なシステム構成になると、複数の監視制御端末と、複数の中央監視装置とをLAN接続し、各監視制御端末配下のドアやセンサのグラフィカルな状態表示及び遠隔操作や、監視制御端末に記録された履歴を定期的に収集し、より大規模な履歴データの保存管理等が可能となる。

【0005】 一方、近年、インターネットを用いた技術が急速に普及している。中でも、WWW(World Wide Web)という情報閲覧技術の利用度は高く、ノートパソコンや携帯情報端末をインターネット上に接続することで、距離に関係なく至る所から情報の発信、取得が容易に可能となる。WWWでは、HTML形式で記述されたテキストをクライアントへ配信し、クライアント側では閲覧用のブラウザを用いて配信されたデータを表示する。

【0006】 また、ASP形式で記述した場合、Webサーバ上で動的にHTMLを生成したり、データベースに接続する機能を備えることができる。

【0007】 より大規模な入室退室管理システムにおいて、離れた地方に点在するビル等を一括管理するような場合、専用ネットワークであるLAN環境では限界があり、インターネット技術の利用は大いに有効かつ必須である。

【0008】 しかし、インターネットを利用した情報のやり取りは、容易な反面、開放度や匿名性が高いため、不正なアクセスに対して発見が難しく、対策が遅れると重大な機密漏洩に繋がる危険性を伴う。

【0009】 入室退室管理システムは上記の様に、機密性の高い場所に対して設置するシステムであり、インターネット上に接続し、情報のやり取りを行うには、不正なアクセスに対して、十分なセキュリティ性が求められることは必至である。

【0010】 上記公報では、インターネットを利用した監視システムにおいて、セキュリティ性を考慮した従来システムが記載されている。

【0011】この従来のシステムでは、クライアント側からサーバ側に対する認証方式として、予め定めたパスワードの照合を用いている。読み込み許可のパスワードと書き込み許可のパスワードの2種類によって、権限の分化を実現している。

【0012】

【発明が解決しようとする課題】第1の問題点は、従来の入退室管理システムでは、中央監視を行える場所が限定的なことである。その理由は、中央監視装置が、入退室管理を行うエリア内に予め設置された専用装置であり、入退室管理システムは専用ネットワークに接続されているため、中央監視装置を遠隔地に設置することは、専用ネットワーク線を引き延ばすことになり、物理的にみて現実的ではないからである。

【0013】第2の問題点は、中央監視装置をインターネット上に接続する場合、クライアント端末からの認証を要しないシステムは不正なアクセスに対して無防備であり、パスワード照合による認証方式を用いた場合でも、十分なセキュリティ性を確保できないことである。その理由は、公的なパスワードを設定した場合、そのパスワードが万一外部に漏れたとき、不正アクセスをされても相手が特定できず発見が困難であり、長期間侵入され続ける恐れがあり、個人毎にパスワードを設定した場合、他人から類推されやすいパスワードが設定される可能性があり、外部から様々な類推パスワードを入力し続ける等の攻撃を受けると簡単にセキュリティが破られる恐れがあるからである。

【0014】第3の問題点は、WebページをHTMLで記述した場合、Webサーバのデータベースをクライアント端末から表示させることが困難である上、十分な保守性が確保できないことである。その理由は、HTMLは、予め用意された静的な情報表示に適したテキスト記述形式で、動的に増減する入退室の履歴を表示させたりする場合、その都度HTMLコードを再生成しなければならないため、複雑なプログラムを要し、メンテナンス効率が低下するからである。

【0015】そこで、本発明の目的は、インターネットを利用した遠隔監視システム及び当該システムに適用される遠隔監視方法において、よりセキュリティ性が高く、保守性に優れた方法及びシステムを提供することにある。

【0016】

【課題を解決するための手段】請求項1記載の発明によれば、管理サーバ端末は、監視制御装置が収集する監視対象物の各種状態変化情報を蓄積し、これと通信接続されたクライアント端末にて前記管理サーバ端末から配信された前記各種状態変化情報を表示することで監視対象物の遠隔監視を行う遠隔監視制御システムにおいて、前記管理サーバ端末と前記クライアント端末をインターネット接続し、ユーザ固有の個人情報を証明書データとし

て書き込んだICカードを発行し、この証明書データを前記管理サーバ端末に送信するICカード発行手段と、前記クライアント端末は、前記ICカードを読みとる手段と、前記管理サーバに対するインターネット接続時にICカードから読みとった証明書データを前記管理サーバに送信する手段とを含み、前記管理サーバは、前記各種状態変化情報に基づきWebページを生成する手段と、前記ICカード発行手段から受信した証明書データに基づき各ユーザに対してアクセス権限を割り当てる手段と、このアクセス権限に基づき前記Webページの配信の可否を決定する手段とを含み、前記クライアント端末より前記ICカードから読みとった証明書データの送信を伴う前記管理サーバに対するインターネット接続が実行されると、前記管理サーバは、受信したユーザの証明書データから前記アクセス権限を参照して当該ユーザに認められるWebページのみを前記クライアント端末に送出することを特徴とする遠隔監視制御システムを得ることができる。

【0017】前記クライアント端末は、前記管理サーバ端末の各Webページへのアクセス要求毎に、前記ICカードから読み込んだ証明書データを前記管理サーバ端末に送信し、前記管理サーバは、受信した証明書データを元に前記アクセス権限を参照することでWebページにアクセスしようとしているユーザを特定し、特定したユーザが、要求されたWebページに対してアクセスを許可されている場合にのみWebページを要求元のクライアント端末に配信するようにしてもよい。

【0018】前記管理サーバ端末から前記クライアント端末に配信されるWebページは、HTML(Hyper Text Markup Language)形式またはASP(Active Server Pages)形式によって記述してもよい。

【0019】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して詳細に説明する。図1に、入退室を監視し管理する遠隔監視制御システムに本発明を適用した実施の形態を表す。Webサーバ15を備えた入退室管理サーバ装置1と、ICカードリーダ7を備えたクライアントWeb端末2と、ICカードリーダライタ8を備えたアクセス制御サーバ装置3と、監視制御端末4と、監視制御端末4に接続され、監視対象となる入退室用ICカードリーダ13a~13n、各カードリーダに接続されるドア14a~14nおよび異常監視用センサ12a~12nからなる。

【0020】入退室管理サーバ1と、クライアントWeb端末2と、アクセス制御サーバ3には、それぞれ表示装置としてディスプレイ9、10、11が接続される。

【0021】入退室管理サーバ1には、ネットワークボードが2枚搭載されており、一方はインターネット5でアクセス制御サーバ3とクライアントWeb端末2に接続され、もう一方はLAN6で監視制御端末4に接続さ

れる。監視制御端末4とカードリーダー13a~13nおよびセンサ12a~12nは通信ライン24で接続される。

【0022】入退室管理サーバ1には、表示プログラム16と、入退室管理プログラム17と、認証プログラム18と、通信プログラム19と、データベース20が実装される。クライアントWeb端末2には、Webブラウザ21と、認証プログラム22と、ICカード読み込みプログラム23が実装される。アクセス制御サーバ3には、表示プログラム25と、アクセス制御プログラム26と、ICカード発行プログラム27と、通信プログラム28が実装される。監視制御端末4には、入退室制御プログラム29と、通信プログラム30と、データベース31が実装される。

【0023】次に、本発明の実施の形態の動作について、図1、図2を参照して詳細に説明する。まず、アクセス制御サーバ3に接続されたICカードライタ8にICカード32を差し込み、証明書発行および入退室管理に必要な個人データ（氏名、会社名、社員番号、役職、所属部署、住所、電話番号、メールアドレス等）を登録すると、ICカード発行プログラム27によりICカード32に証明書データと入退室管理データが書き込まれる。

【0024】登録時に、予め設定されたグループ分けの方法（役職毎、所属部署毎等）によって、WebページのURL（Uniform Resource Identifiers）毎にアクセス権限の有無が設定され、アクセス制御プログラム26によりアクセス制御リスト33として生成され、通信プログラム28によりインターネット5を介して入退室管理サーバ1に配布され、入退室管理サーバ1では通信プログラム19によりアクセス制御リスト33を受信し、データベース20に保存する。

【0025】発行したICカード32を、監視制御端末4配下のICカードリーダー13a~13nに読み込ませることで、入退室制御プログラム29によるドア14a~14nの開閉、データベース31への入退室履歴の記録等が行われる。

【0026】監視制御端末4は、入退室制御プログラム29によりカードリーダー13a~13n、ドア14a~14nやセンサ12a~12nの状態変化を収集し、通信プログラム30によってリアルタイムに入退室管理サーバ1に送信する。

【0027】入退室管理サーバ1は監視制御端末4から送信された状態情報を通信プログラム19により受信し、表示プログラム16によりディスプレイ9に表示する。また入退室管理プログラム17により定期的に監視制御端末4のデータベース31から入退室等の履歴を収集し、データベース20に保存する。保存されたデータベース20は、表示プログラム16によりディスプレイ9上での閲覧、検索ができる。

【0028】クライアントWeb端末2による遠隔監視

を行う場合、発行したICカード32を、クライアントWeb端末2に接続されたICカードリーダー7に差し込み、Webブラウザ21により、インターネット5を介して入退室管理サーバ1のWebサーバ15に対し表示したい情報のWebページ34URLを要求する。

【0029】Webサーバ15へWebページ34を要求するとき、クライアントWeb端末2は、ICカード読み込みプログラム23によりICカード32からカード内データを読み込み、認証プログラム22により証明書データを取り出し、Webブラウザ21によりインターネット5を介して入退室管理サーバ1に対して認証要求を送信する。

【0030】入退室管理サーバ1は、通信プログラム19により認証要求を受信し、認証プログラム18により、アクセス制御リスト33を基に要求元のユーザに対し、要求されたURLのWebページ34へのアクセスを許可するか拒否するかを判断する。

【0031】アクセス許可の場合は、Webサーバ15によりクライアントWeb端末2から要求された情報を元にASP形式のWebページ34を生成し、インターネット5を介してWebページ34をクライアントWeb端末2に配信する。

【0032】アクセス拒否の場合は、権限がない旨を伝えるメッセージをHTML形式にしてクライアントWeb端末2に配信する。

【0033】次に、本発明の実施例について図面を参照して詳細に説明する。図3を参照すると、本発明の実施例は、エリアA36a、エリアB36bからなるプラント35における入退室管理システムを示している。エリアA36aは部門A37aが使用しており、入り口にICカードリーダー13aとドア14aが設置されている。エリアB36bは部門B37bが使用しており、入り口にICカードリーダー13bとドア14bが設置されている。

【0034】ICカードリーダー13a、13bは通信ライン24により監視制御端末4に接続され、監視制御端末4はLAN6により入退室管理サーバ1に接続されている。

【0035】入退室管理サーバ1はインターネット5に接続され、インターネット5上には、ICカードライタ8を備えたアクセス制御サーバ3と、ICカードリーダー7を備えたクライアントWeb端末2が接続されている。

【0036】また、部門A37aにはICカード32を所持した管理者A42が所属している。

【0037】次に、本発明の実施例の動作について、図3、4を参照して詳細に説明する。図3、図4を参照すると、まず、部門A37aに所属する管理者A42が、アクセス制御サーバ3に接続されたICカードライタ8にICカード32を差し込み、個人データを登録すると、入退室管理サーバのデータベース20に個人データ

が登録される。また入退室に必要なデータおよび証明書データが書き込まれたＩＣカード３２が発行される。

【００３８】管理者Ａ４２は、ＩＣカード３２をカードリーダー１３ａに読み込ませることにより、ドア１４ａから入室することができるようになる。また、管理者Ａ４２は、プラント３５内にいないときでも、ＩＣカード３２をクライアントＷｅｂ端末２に接続されたＩＣカードリーダー７に差し込み、入退室管理サーバ１上のＷｅｂサーバ１５にアクセスすることで、エリアＡ３６ａのエリアＡ監視画面３４ａや、入退室履歴の参照ができ、必要に応じてドア１４ａの開閉を遠隔操作することも可能である。

【００３９】ドアからの入室権限を部門毎に設定した場合、部門Ａ３７ａの所属である管理者Ａ４２は、部門Ｂ３７ｂのドア１４ｂから入室することはできない。Ｗｅｂページへのアクセス権限を部門毎に設定した場合、部門Ａ３７ａの所属である管理者Ａ４２は、部門Ｂ３７ｂのエリアＢ監視画面３４ｂを参照、操作することはできない。

【００４０】管理者Ａ４２が、部門Ａ３７ａから部門Ｂ３７ｂに所属替えになった場合でも、アクセス制御サーバ３から個人データを変更し、管理者Ａ４２の所属を部門Ｂ３７ｂに変更することで、管理者Ａ４２は、ドア１４ｂからの入室およびエリアＢ監視画面３４ｂへのアクセスができるようになり、ドア１４ａからの入室およびエリアＡ監視画面３４ａへのアクセスはできなくなる。

【００４１】管理者Ａ４２がＩＣカード３２を紛失あるいは盗難にあった場合でも、アクセス制御サーバ３から、管理者Ａ４２の権限を変更することで、ＩＣカード３２を用いた不正入室や、Ｗｅｂサーバ１５への不正アクセスを即座に防止することができる。

【００４２】仮に、Ｗｅｂページへのアクセスがパスワードによる認証方式であった場合、パスワードを盗まれても、不正アクセスされていることに、システム管理者が気づかない限り、盗まれたパスワードによるアクセスを防止することができない。

【００４３】また、クライアントＷｅｂ端末２からＷｅｂサーバ１５への、証明書によるクライアント認証要求をする前に、パスワードによる照合を設けることもできる。

【００４４】パスワード照合と証明書による認証とを併用することで、よりセキュリティの向上を図ることができる。入退室管理システムにおいて、遠隔地からでも状態監視が可能になることである。

【００４５】本実施の形態のように、インターネット上に入退室管理サーバ装置を設置し、入退室サーバ装置にＷｅｂサーバ手段を持たせることで、クライアントＷｅｂ端末をインターネット上に接続すれば、どこからでも入退室管理サーバ装置のＷｅｂサーバにアクセスすることができ、大規模な監視制御システムであっても、遠隔

地から容易に監視することができる。

【００４６】また、インターネットを利用した遠隔状態監視システムでは、セキュリティ面において問題を有していたが、ＩＣカード内の証明書データを用いたクライアント認証システムと、アクセス制御リストを用いることで、個人毎に各Ｗｅｂページのアクセス制限の設定及び管理を可能とし、高いセキュリティを確保することができる。ＩＣカードが紛失あるいは盗難された場合でも、システム管理者に知らせることで即座に不正なアクセスを防止することもできる。

【００４７】更に、インターネットを利用した遠隔状態監視システムにおいて、高い保守性を確保することができる。ＷｅｂページをＡＳＰ形式で記述することで、中央監視装置のデータベースへのアクセスが容易となり、表示項目の追加、変更等が短期間でできるからである。

【００４８】次に、本発明の第２の実施の形態について図面を参照して説明する。図１、図５を参照すると、本発明の第２の実施の形態は、ＩＣカード３２の代わりに非接触カード４０を、入退用ＩＣカードリーダー１３ａ～１３ｎの代わりに非接触カードリーダー４１ａ～４１ｎを、クライアントＷｅｂ端末２に接続するＩＣカードリーダー７の代わりに非接触カードリーダー３８を、アクセス制御サーバ３に接続するＩＣカードライタ８の代わりに非接触カードライタ３９を使用する点で第１の実施の形態と異なる。

【００４９】

【発明の効果】以上、本発明によれば、インターネットを利用した遠隔監視制御システムであっても、高いセキュリティを確保した遠隔監視システム及びその方法を得ることができ、保守性に優れた効果を有する。

【図面の簡単な説明】

【図１】発明の第１の実施の形態の全体構成を示すブロック図である。

【図２】本発明の第１の実施の形態の動作を示すブロック図である。

【図３】本発明の第１の実施の形態の具体的な実施例の構成を示すブロック図である。

【図４】本発明の第１の実施の形態の具体的な実施例の動作を示すブロック図である。

【図５】本発明の第２の実施の形態の構成を示すブロック図である。

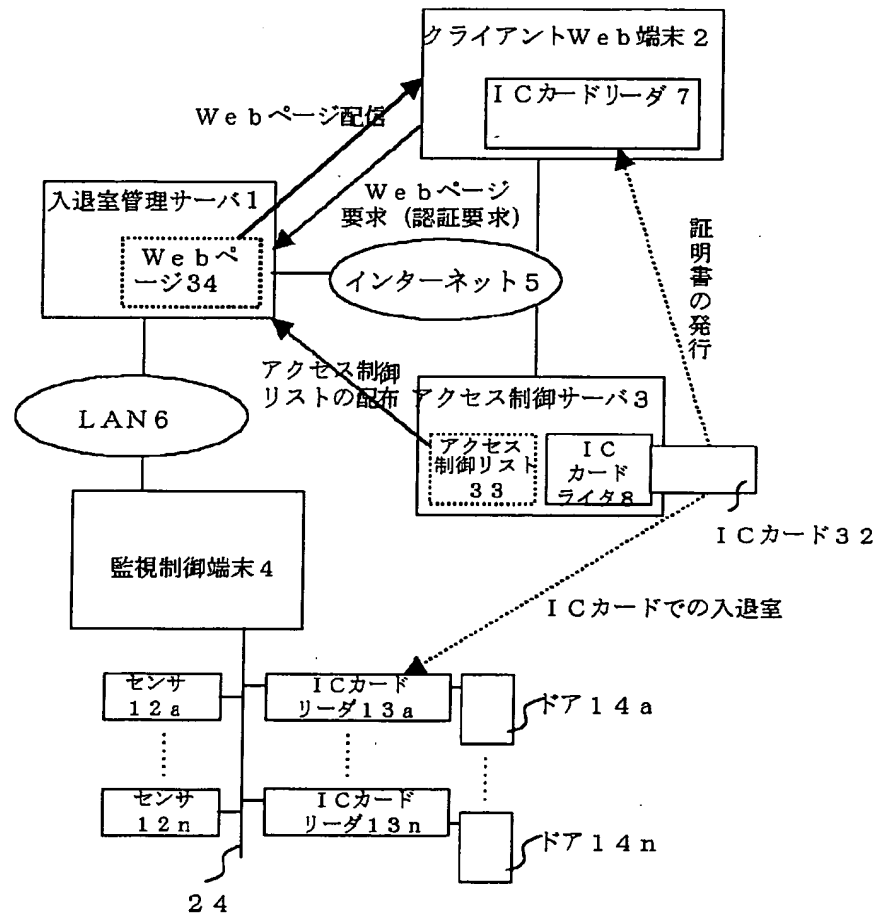
【符号の説明】

- １ 退室管理サーバ
- ２ クライアントＷｅｂ端末
- ３ アクセス制御サーバ、
- ４ 監視制御端末
- ５ インターネット
- ６ ＬＡＮ
- ７ ＩＣカードリーダー
- ８ ＩＣカードライタ

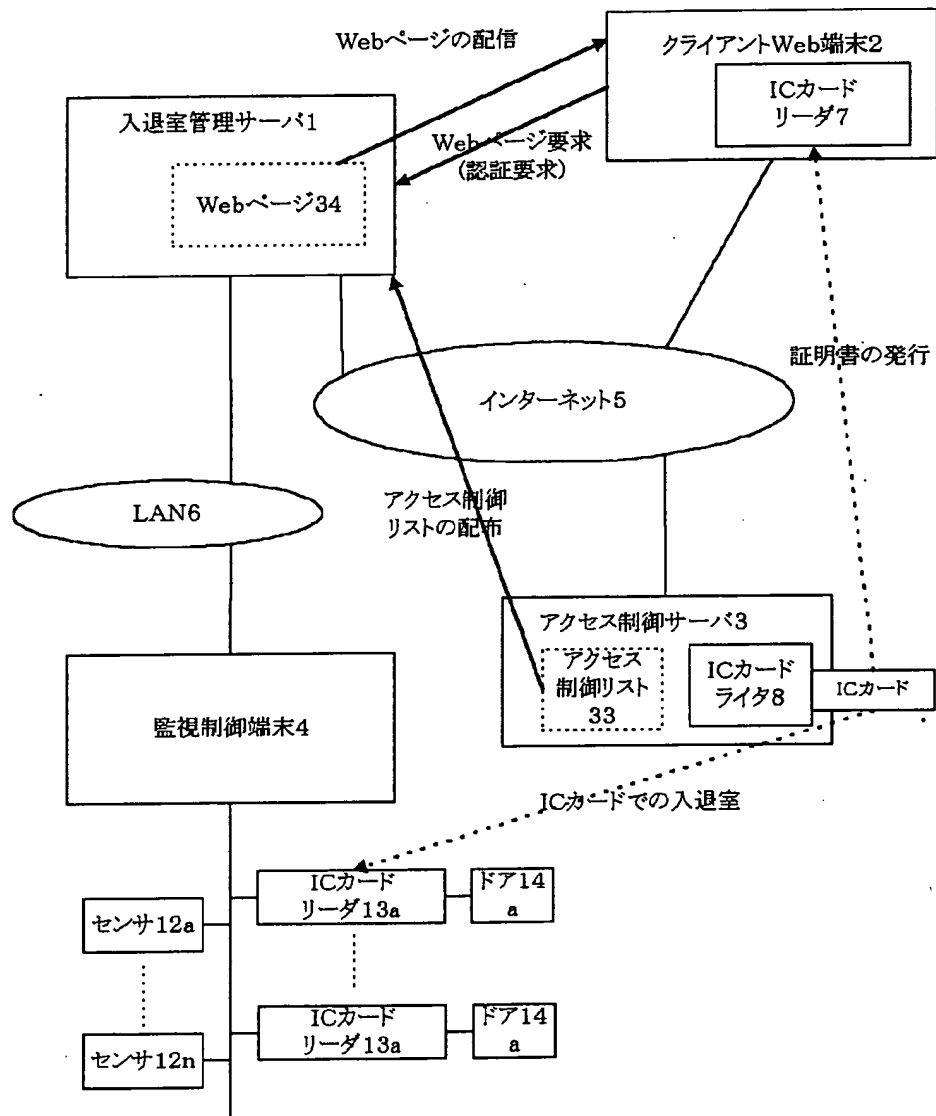
9～11 ディスプレイ
 12 センサ
 13 入退用ICカードリーダー
 14 ドア
 15 Webサーバ
 16 表示プログラム
 17 入退室管理プログラム
 18 認証プログラム
 19 通信プログラム
 20 データベース
 21 Webブラウザ
 22 認証プログラム
 23 ICカード読込プログラム
 24 通信ライン
 25 表示プログラム
 26 アクセス制御プログラム

27 ICカード発行プログラム
 28 通信プログラム
 29 入退室制御プログラム
 30 通信プログラム
 31 データベース
 32 ICカード
 33 アクセス制御リスト
 34 Webページ
 35 プラント
 36 エリア
 37 部門
 38 非接触カードリーダー
 39 非接触カードライタ
 40 非接触カード
 41 入退用非接触カードリーダー
 42 管理者A

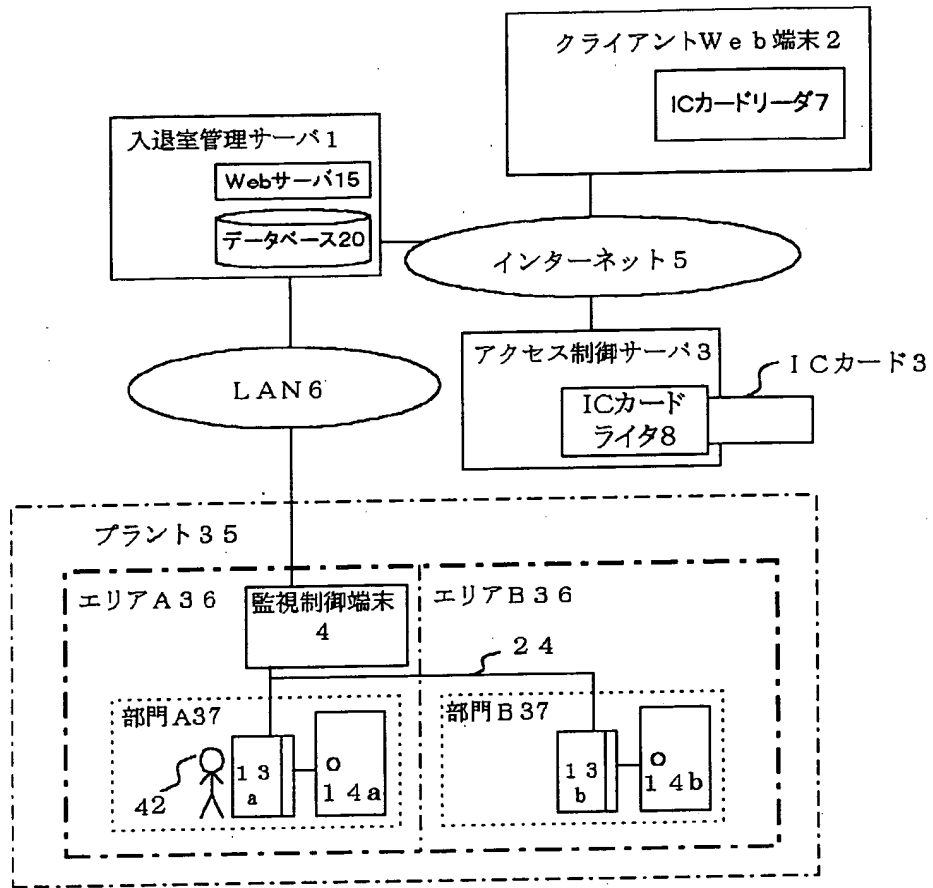
【図2】



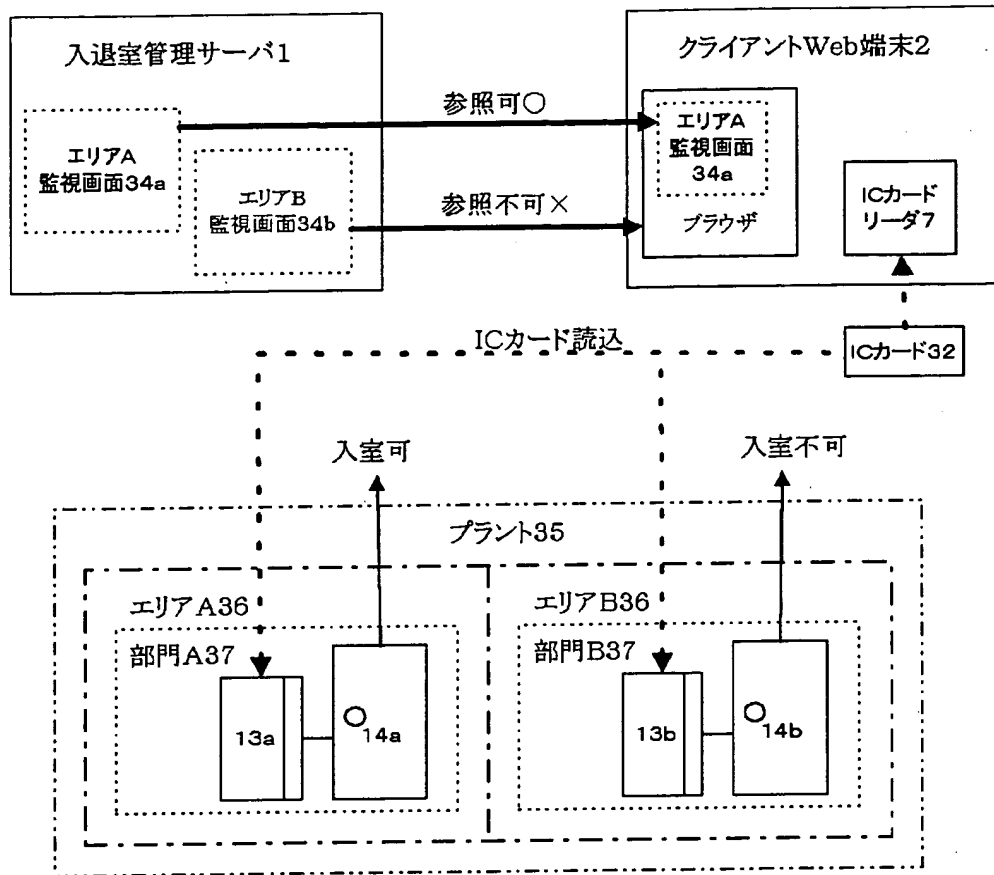
【図1】



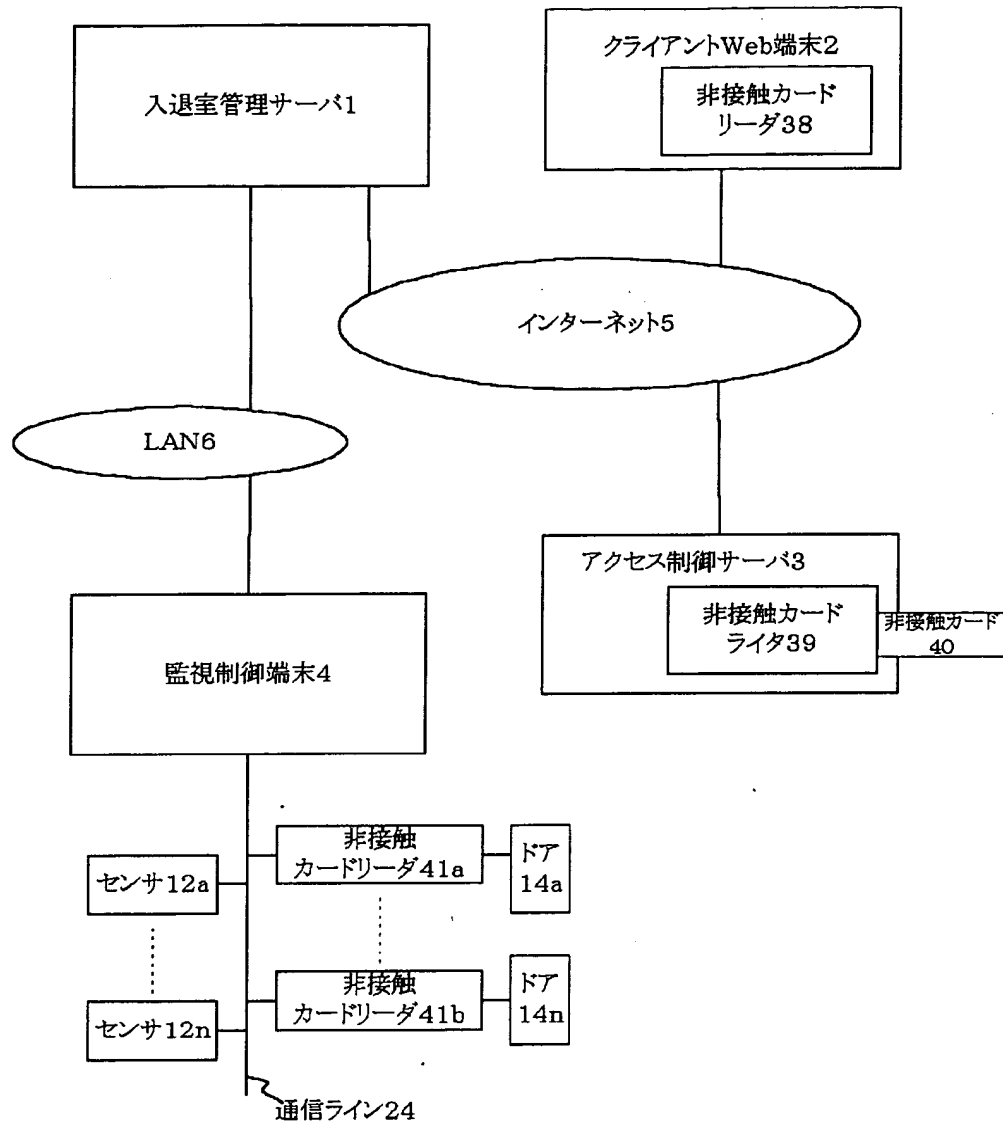
【図3】



【図4】



【図5】



フロントページの続き

Fターム(参考) 5B058 CA27 KA31
 5C087 AA02 AA03 BB12 BB74 DD06
 EE02 EE08 FF01 FF04 GG66
 GG70 GG83
 5K048 AA15 BA51 BA53 BA55 DC07
 EA16 EB02 HA01 HA02
 5K101 KK11 LL01



(19)

(11) Publication number: **2002281:**

Generated Document.

PATENT ABSTRACTS OF JAPAN(21) Application number: **2001078703**(51) Intl. Cl.: **H04Q 9/00 G06K 17/00 G08B 25/04**
11/00(22) Application date: **19.03.01**

(30) Priority:

(43) Date of application
publication: **27.09.02**(84) Designated contracting
states:(71) Applicant: **NEC ENG LTD**(72) Inventor: **SHIMAZU NORIHIKO**

(74) Representative:

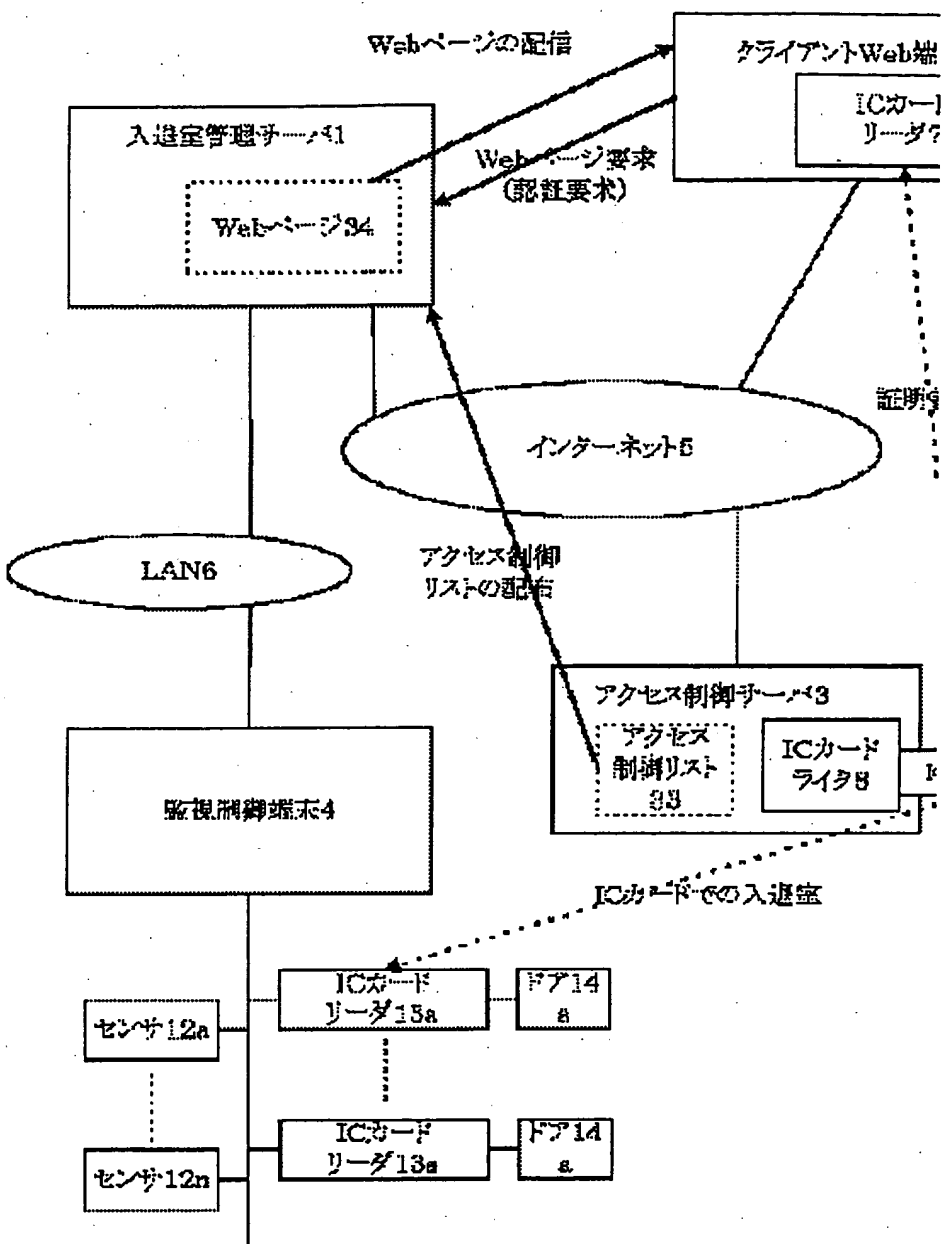
**(54) REMOTE MONITORING
METHOD AND SYSTEM
USING INTERNET**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide an entering/leaving management system capable of monitoring a state from a remote place and preventing a client device from illicitly accessing a server device and having high security.

SOLUTION: The entering/leaving management server is installed with a Web server and is connected to the Internet to realize remote state monitoring from a client Web terminal. A certificate in an IC card is used for the client authentication from the client Web terminal to the Web server, whereby improving security for illicit access.

COPYRIGHT: (C)2002,JPO



THOMSON

DELPHION

RESEARCH

PRODUCTS

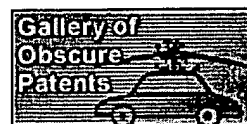
INSIDE DELPHION

[Log Out](#) | [Work Files](#) | [Saved Searches](#) | [My Account](#) | [Products](#)Search: [Quick/Number](#) [Boolean](#) [Advanced](#) [Derwent](#)

The Delphion Integrated View

Buy Now: ☒ PDF | [More choices...](#)Tools: [Annotate](#) | Add to Work File: [Create new Work File](#)View: [INPADOC](#) | Jump to: [Top](#)[Email this to a](#)Title: **JP2002281573A2: REMOTE MONITORING METHOD AND SYSTEM USING INTERNET**Country: **JP Japan**Kind: **A2 Document Laid open to Public inspection**Inventor: **SHIMAZU NORIHIKO;**Assignee: **NEC ENG LTD**
[News, Profiles, Stocks and More about this company](#)Published / Filed: **2002-09-27 / 2001-03-19**Application Number: **JP2001000078703**IPC Code: **H04Q 9/00; G06K 17/00; G08B 25/04; H04M 11/00;**Priority Number: **2001-03-19 JP2001000078703**Abstract: **PROBLEM TO BE SOLVED:** To provide an entering/leaving management system capable of monitoring a state from a remote place and preventing a client device from illicitly accessing a server device and having high security.**SOLUTION:** The entering/leaving management server is installed with a Web server and is connected to the Internet to realize remote state monitoring from a client Web terminal. A certificate in an IC card is used for the client authentication from the client Web terminal to the Web server, whereby improving security for illicit access.

COPYRIGHT: (C)2002,JPO

Family: **None**Other Abstract Info: **DERABS G2003-079971**[Nominate](#)[this for the Gallery...](#)

© 1997-2004 Thomson

[Research Subscriptions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Site Map](#) | [Contact Us](#) | [Help](#)